



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/667,090	09/21/2000	Messaoud Benantar	AUS9-2000-0255-US1	6109

7590 12/31/2003
Joseph R Burwell
Law Office of Joseph R Burwell
P O Box 28022
Austin, TX 78755-8022

EXAMINER

OSMAN, AHMED A

ART UNIT PAPER NUMBER

2136

DATE MAILED: 12/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/667,090

Applicant(s)

BENANTAR ET AL.

Examiner

Ahmed A Osman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 18 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED OFFICE ACTION

1. Claims 1 – 40 are presented for examinations.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-7, 9, and 11-13 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by US Patent No. 6,233,577 to Ramasubramani.

As per claim 1:

“Receiving a digital certificate from the client at a host within the distributed data processing system”

Ramasubramani teaches a centralized certificate management system for two-way interactive communication devices in data networks (Column 3 Line 20) that resembles a data processing system coupled to a network (Column 3 Line 16).

Art Unit: 2136

Ramasubramani further teaches an example where a user sends a message to a merchant web site, he signs it with his digital ID to assure the recipient that the message was actually sent by him (Column 4 Line 17). Ramasubramani later teaches that the most secure use of authentication involves enclosing one or more certificates with every message and the receiver of the message would verify the certificate (Column 4 Line 29).

“Obtaining a host identity for the client from the digital certificate”

Ramasubramani teaches that digital certificates contain digital signature of the certificate issuer (Column 3 Line 57).

“Retrieving host-encrypted secret data associated with the host identity from the digital certificate.

Decrypting the host-encrypted secret data with a host private key”

Ramasubramani teaches that a digital certificate contains an expiration date, name of the certifying authority that issued the certificate, a serial number and other information. Ramasubramani further states that more importantly it contains the digital signature of the certificate issuer, i.e. encrypted “fingerprint” that can be used to verify the contents of the certificate (Column 3 Line 54). Ramasubramani further states that the digital certificate is issued by a Certifying authority and signed with the CA’s private key (Column 3 Line 60). Moreover Ramasubramani discloses that digital certificate uses public key encryption techniques that are based on a pair of related keys, a public

key and a private key (Column 3 Line 66). Ramasubramani also states that the public key is used to verify a message signed the private key or encrypt messages that can only be decrypted using the private key (Column 4 Line 3). Ramasubramani finally teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31). Examiner concludes that the process of receiving the request for a certificate by the CA involves retrieving and decrypting the data that was originally signed and encrypted by the CA, in other words retrieving and decrypting the CA-encrypted secret data.

“Authenticating the client using the host identity and decrypted secret data”

Figure 1 of Ramasubramani clearly illustrates the client authentication process.

As per claim 2:

“Wherein the host acts a s proxy for the client”

Ramasubramani teaches a proxy server computer 114 that performs data communication (Column 5 Line 18).

As per claim 3:

“Verifying the received digital certificate”

Ramasubramani teaches that the receiver of the message would verify the certificate using the certifying authority’s public key (Column 4 Line 31).

As per claim 4:

“Generating, at the client, a request for a digital certificate comprising host identity mapping data;

Ramasubramani teaches a certificate engine 402 that uses the generated distinguished name and public key obtained from a key generator 412 to generate a certificate signing request or CSR. Ramasubramani further states that the CSR is a public standard format for requesting certificates from a Certifying Authority (CA) (Column 11 Line 21).

“Sending the request for the digital certificate to a certifying authority (CA)”

Ramasubramani teaches that the CSR is a binary block of data packaged in a certificate request in a standard form that is then sent to the CA (Column 11 Line 28).

“Receiving a digital certificate comprising host identity mapping data from the certificate authority”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31). Ramasubramani further teaches that when the certificate response comes back from the CA, the certificate engine extracts the distinguished information from the received certificate (Column 11 Line 38).

As per claim 5:

**“Storing the host identity in the request for the digital certificate.
Encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data.
Storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate”**

Ramasubramani teaches that a digital certificate contains an expiration date, name of the certifying authority that issued the certificate, a serial number and other information. Ramasubramani further states that more importantly it contains the digital signature of the certificate issuer, i.e. encrypted “fingerprint” that can be used to verify

Art Unit: 2136

the contents of the certificate (Column 3 Line 54). Ramasubramani further states that the digital certificate is issued by a Certifying authority and signed with the CA's private key (Column 3 Line 60). Moreover Ramasubramani discloses that digital certificate uses public key encryption techniques that are based on a pair of related keys, a public key and a private key (Column 3 Line 66). Ramasubramani also states that the public key is used to verify a message signed the private key or encrypt messages that can only be decrypted using the private key (Column 4 Line 3). Ramasubramani finally teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31). Examiner concludes that the process of receiving the request for a certificate by the CA involves retrieving and decrypting the data that was encrypted and stored in the request for certificate, in other words retrieving and decrypting the CA-encrypted secret data. In order for that step to occur, a prior procedure that encrypts and stores the CA data in the request had to take place.

As per claim 6:

“Receiving, at the certifying authority, the request for a digital certificate”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing

Art Unit: 2136

the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31).

“Generating the digital certificate in response to the received request for the digital certificate”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31).

“Sending the generated digital certificate to the client”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31).

As per claim 7:

“Retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate.

Decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted data.

Encrypting the decrypted secret data associated with the host identity using a public key of the host to generate host-encrypted secret data.

Storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate”

Ramasubramani teaches that a digital certificate contains an expiration date, name of the certifying authority that issued the certificate, a serial number and other information. Ramasubramani further states that more importantly it contains the digital signature of the certificate issuer, i.e. encrypted “fingerprint” that can be used to verify the contents of the certificate (Column 3 Line 54). Ramasubramani further states that the digital certificate is issued by a Certifying authority and signed with the CA's private key (Column 3 Line 60). Moreover Ramasubramani discloses that digital certificate uses public key encryption techniques that are based on a pair of related keys, a public key and a private key (Column 3 Line 66). Ramasubramani also states that the public key is used to verify a message signed the private key or encrypt messages that can only be decrypted using the private key (Column 4 Line 3). Ramasubramani finally teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31). Examiner concludes that the process of receiving the request for a certificate by the CA involves retrieving and decrypting the data that was originally signed and encrypted by the CA, in other words retrieving and decrypting the CA-encrypted secret

Art Unit: 2136

data. Examiner also concludes that the process of issuing a certificate by the CA involves encrypting the CA's digital signature and storing it in the digital certificate to be issued.

As per claim 9:

“Wherein the digital certificate is formatted according to the X.509 standard.”

Ramasubramani teaches that the most widely accepted format for digital certificates is defined the CCITT X.509 international standard (Column 3 Line 62).

As per claim 11:

“Performing multiple authentication processes within the distributed data processing system for the client through the host using information within the digital certificate.”

Figure 1 of Ramasubramani clearly illustrates the client authentication process.

As per claim 12:

“Receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31).

“Generating the digital certificate in response to the received request for a digital certificate”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31).

“Sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.”

Ramasubramani teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing

Art Unit: 2136

the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31).

As per claim 13:

“Retrieving CA-encrypted secret data from the host identity mapping data in the request for a digital certificate.

Decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data.

Encrypting the decrypted secret data associated with the host identity using a public key of a host to generate a host-encrypted secret data.

Storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate”

Ramasubramani teaches that a digital certificate contains an expiration date, name of the certifying authority that issued the certificate, a serial number and other information. Ramasubramani further states that more importantly it contains the digital signature of the certificate issuer, i.e. encrypted “fingerprint” that can be used to verify the contents of the certificate (Column 3 Line 54). Ramasubramani further states that the digital certificate is issued by a Certifying authority and signed with the CA’s private

Art Unit: 2136

key (Column 3 Line 60). Moreover Ramasubramani discloses that digital certificate uses public key encryption techniques that are based on a pair of related keys, a public key and a private key (Column 3 Line 66). Ramasubramani also states that the public key is used to verify a message signed the private key or encrypt messages that can only be decrypted using the private key (Column 4 Line 3). Ramasubramani finally teaches that upon receiving the certificate request, the CA verifies the supplied information therein and attests to the validity of the user by signing the certificate and then issues a certificate response, which contains the signed certificate (Column 11 Line 31). Examiner concludes that the process of receiving the request for a certificate by the CA involves retrieving and decrypting the data that was originally signed and encrypted by the CA, in other words retrieving and decrypting the CA-encrypted secret data. Examiner also concludes that the process of issuing a certificate by the CA involves encrypting the CA's digital signature and storing it in the digital certificate to be issued.

4. Claim 40 is rejected under 35 U.S.C. 102(e) as being clearly anticipated by US Patent No. 6,324,645 to Andrews.

As per claim 40:

“A data structure representing a digital certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a subject name;

an extension,

wherein the extension comprises a host identity and host-encrypted secret data associated with the host identity.”

Andrews clearly illustrates in Figure 2 the preferred embodiment of the digital certificate discussed in the disclosed invention (Column 4 Line 18). Andrews teaches that each digital certificate issued by the CA is provided a unique serial number (Column 9 Line 30). Therefore the CA is the issuer of each digital certificate. Andrews further teaches that the digital certificate, which uses the X.509 format, includes the CA's distinguished name (Column 9 Line 23). Moreover, Andrews teaches that the digital certificate includes the user's distinguished name and the CA's digital signature (Column 9 Line 25). Finally Andrews teaches that the digital certificate includes digital certificate extensions. Andrews further states that the digital certificate extensions are proprietary, published extensions following the X.509 convention and include an access label, which is used to signal the authority granted to the user (Column 9 Line 36). Andrews later states that the Access labels include a domain identifier, which identifies the domain which the user may access (Column 9 Line 53). Furthermore Andrews teaches that the access label is a one-way hash of the organization name, which shall

Art Unit: 2136

be referred to as a jurisdiction hash (Column 9 Line 59). Examiner concludes that the extensions contain the host identity.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,233,577 to Ramasubramani as applied to claims 1-7, 9, and 11-13 above, and further in view of US Patent No. 6,324,645 to Andrews.

As per claim 8:

“Wherein the digital certificate comprise multiple host identities for multiple hosts within the distributed data processing system.”

Ramasubramani fails to state that the digital certificate may contain multiple host identities. Andrews teaches in the disclosed invention a digital certificate that uses the X.509 format and includes possibly digital certificate extensions and the Certifying

Art Unit: 2136

Authority's (CA) digital signature (Column 9 Line 24). Andrews further states that the digital certificate extensions are proprietary, published extensions following the X.509 convention and include an access label, which is used to signal the authority granted to the user (Column 9 Line 36). Andrews later states that the Access labels include a domain identifier, which identifies the domain which the user may access (Column 9 Line 53). Furthermore Andrews teaches that the access label is a one-way hash of the organization name, which shall be referred to as a jurisdiction hash (Column 9 Line 59). Andrews also states that the access label may include multiple jurisdiction hashes to accommodate users who belong to more than one organization (Column 10 Line 8). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ramasubramani's invention to enable the digital certificate to include multiple host identities. One would have been motivated to do so in light of Andrews' teachings that including multiple jurisdiction hashes accommodates users who belong to more than one organization (Column 10 Line 8).

As per claim 10:

“Wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.”

Ramasubramani fails to state in the disclosed invention that a host identity is stored in the extension of the X.509 formatted digital certificate. Andrews teaches in the disclosed invention a digital certificate that uses the X.509 format and includes possibly digital certificate extensions and the Certifying Authority's (CA) digital signature (Column 9 Line 24). Andrews further states that the digital certificate extensions are proprietary, published extensions following the X.509 convention and include an access label, which is used to signal the authority granted to the user (Column 9 Line 36). Andrews later states that the Access labels include a domain identifier, which identifies the domain which the user may access (Column 9 Line 53). Furthermore Andrews teaches that the access label is a one-way hash of the organization name, which shall be referred to as a jurisdiction hash (Column 9 Line 59). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ramasubramani's invention to enable the digital certificate to include the host identity in the extension of the X.509 formatted digital certificate. One would have been motivated to make such a modification in light of Andrews' teachings that use of digital certificates is advantageous to enable establishment of the user's identity and the user's authorized domain and/or privilege and is more secure than using passwords (Column 3 Line 61). Andrews further teaches that the use of access labels for this purpose is a flexible approach, which supports the implementation of a wide variety of risk management policies (Column 4 Line 2).

7. Regarding claims 14-26

Ramasubramani states that in the detailed description of the disclosed invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will become obvious to those skilled in the art that the present invention may be practiced without these specific details. In other instances, well known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the present invention. The detailed description of the present invention in the following are presented largely in terms of procedures, steps, logic blocks, processing, and other symbolic representations that resemble of data processing devices coupled to networks. These process descriptions and representations are the means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. The present invention is a centralized certificate management system for two-way interactive communication devices in data networks. The method along with the architecture to be described in detail below is a self-consistent sequence of processes or steps leading to a desired result. These steps or processes are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities may take the form of electrical signals capable of being stored, transferred, combined, compared, displayed and otherwise manipulated in a computer system or electronic computing devices. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, operations, messages, terms, numbers, or the like. It should be borne in mind that all of these similar terms are to be associated with the appropriate physical quantities and are merely convenient labels

Art Unit: 2136

applied to these quantities. Unless specifically stated otherwise as apparent from the following description, it is appreciated that throughout the present invention, discussions utilizing terms such as "processing" or "computing" or "verifying" or "displaying" or the like, refer to the actions and processes of a computing device that manipulates and transforms data represented as physical quantities within the computing device's registers and memories into other data similarly represented as physical quantities within the computing device or other electronic devices (Column 3 Line 4).

Examiner interprets that the disclosed invention includes means or an apparatus to carry out the method or process in the disclosed invention. Therefore:

As per claim 14:

The rationale used in the rejection of claim 1 is incorporated in the rejection for this claim.

As per claim 15:

The rationale used in the rejection of claim 2 is incorporated in the rejection for this claim.

As per claim 16:

The rationale used in the rejection of claim 3 is incorporated in the rejection for this claim.

As per claim 17:

The rationale used in the rejection of claim 4 is incorporated in the rejection for this claim.

As per claim 18:

The rationale used in the rejection of claim 5 is incorporated in the rejection for this claim.

As per claim 19:

The rationale used in the rejection of claim 6 is incorporated in the rejection for this claim.

As per claim 20:

The rationale used in the rejection of claim 7 is incorporated in the rejection for this claim.

As per claim 21:

The rationale used in the rejection of claim 8 is incorporated in the rejection for this claim.

As per claim 22:

The rationale used in the rejection of claim 9 is incorporated in the rejection for this claim.

As per claim 23:

The rationale used in the rejection of claim 10 is incorporated in the rejection for this claim.

As per claim 24:

The rationale used in the rejection of claim 11 is incorporated in the rejection for this claim.

As per claim 25:

The rationale used in the rejection of claim 12 is incorporated in the rejection for this claim.

As per claim 26:

The rationale used in the rejection of claim 13 is incorporated in the rejection for this claim.

8. Regarding claims 27-39

Ramasubramani states that Appendix A, which is a part of the present disclosure, is a microfiche appendix entitled "Centralized Certificate Management System for Two-way Communication Devices in Data Networks" consisting of 2 sheets of microfiche having a total of 184 frames. The microfiche Appendix is a source code listing of one embodiment of the centralized certificate management system for two-way interactive communication devices over a wireless data network in the present invention, which is described more completely below (Column 1 Line 8).

Examiner concludes that Appendix A contains source code or software that would provide instructions to a computer to carry out the discussed method or process.

Therefore:

As per claim 27:

The rationale used in the rejection of claim 1 is incorporated in the rejection for this claim.

As per claim 28:

The rationale used in the rejection of claim 2 is incorporated in the rejection for this claim.

As per claim 29:

Art Unit: 2136

The rationale used in the rejection of claim 3 is incorporated in the rejection for this claim.

As per claim 30:

The rationale used in the rejection of claim 4 is incorporated in the rejection for this claim.

As per claim 31:

The rationale used in the rejection of claim 5 is incorporated in the rejection for this claim.

As per claim 32:

The rationale used in the rejection of claim 6 is incorporated in the rejection for this claim.

As per claim 33:

The rationale used in the rejection of claim 7 is incorporated in the rejection for this claim.

As per claim 34:

The rationale used in the rejection of claim 8 is incorporated in the rejection for this claim.

As per claim 35:

The rationale used in the rejection of claim 9 is incorporated in the rejection for this claim.

As per claim 36:

The rationale used in the rejection of claim 10 is incorporated in the rejection for this claim.

As per claim 37:

The rationale used in the rejection of claim 11 is incorporated in the rejection for this claim.

As per claim 38:

The rationale used in the rejection of claim 12 is incorporated in the rejection for this claim.

As per claim 39:

The rationale used in the rejection of claim 13 is incorporated in the rejection for this claim.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

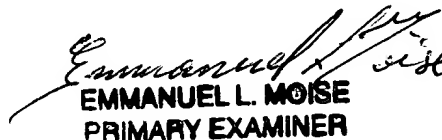
The following patents are cited to further show the state of the art with respect to cryptographic key processing in general:

U.S. Patent No. 4,868,877 to Fischer
U.S. Patent No. 5,371,794 to Diffie et al.
U.S. Patent No. 5,712,914 to Aucsmith et al.
U.S. Patent No. 5,774,552 to Grimmer
U.S. Patent No. 5,982,898 to Hsu et al.
U.S. Patent No. 6,026,166 to LeBourgeois
U.S. Patent No. 6,189,097 to Tycksen Jr. et al.
U.S. Patent No. 6,230,266 to Perlman et al.
U.S. Patent No. 6,301,658 to Koehler
U.S. Patent No. 6,321,333 to Murray
U.S. Patent No. 6,341,351 to Muralidhran et al.
U.S. Patent No. 6,405,313 to Reiter et al.
U.S. Patent No. 6,553,493 to Okumura
U.S. Patent No. 6,564,320 to de Silva et al.
U.S. Patent No. 6,584,565 to Zamek

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmed A Osman whose telephone number is 703-305-8910. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.


EMMANUEL L. MOISE
PRIMARY EXAMINER

Ahmed Osman

United States Patent & Trademark Office

Patent Examiner – AU 2136

December 22, 2003